

UNDER SEAL

II. PURPOSE OF THE AFFIDAVIT

4. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachments A, B, and C** of this Affidavit. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts that I believe are necessary to establish probable cause for a search warrant for the person of Ryan Christopher Ramos, DOB: 10/22/1985 (the **SUBJECT PERSON**), the residence located at 1020 Luxe Ave, Apt #8410, Columbus, OH 43220 (the **SUBJECT PREMISES**); and the vehicle belonging to the **SUBJECT PERSON**, specifically a Toyota Rav4, VIN 2T3P1RFV2NW306767, with Ohio license plate number HLH2747 (the **SUBJECT VEHICLE**). I have not omitted any facts that would negate probable cause
5. The **SUBJECT PREMISES**, **SUBJECT VEHICLE**, and **SUBJECT PERSON**, to be searched are more particularly described in **Attachment A** and **B** respectively, for the items specified in **Attachment C**, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252, and 2252A – the distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the **SUBJECT PERSON**, **SUBJECT VEHICLE**, and the entire **SUBJECT PREMISES**, including the residential dwelling, curtilage, detached buildings and storage units, for any computers, cellular “smart” phones and/or mobile computing device or digital media located thereon/therein, and to thereafter seize and examine any such device that is recovered from the **SUBJECT PERSON**, **SUBJECT VEHICLE** or **SUBJECT PREMISES**, for items specified in **Attachment C**, and to seize all items listed in **Attachment C** as evidence, fruits, and instrumentalities of the above violations.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or

possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

7. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
8. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
9. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”² is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture,

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and **Attachments A and B** hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §2252 and child pornography as defined in 18 U.S.C. § 2256(8).

² The term child pornography is used throughout this affidavit. All references to this term in this affidavit and **Attachments A and B** hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §2252 and child pornography as defined in 18 U.S.C. § 2256(8).

or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

10. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.
11. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”
12. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.
13. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
14. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) and 2256(6) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
15. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic

form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

16. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.
17. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
18. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
19. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples

include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND MOBILE APPLICATIONS

20. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
21. Computers, mobile devices, and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
22. Computers, tablets, and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a hard copy photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.
23. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such

computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

24. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 128 Gigabytes. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 32 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 32 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.
25. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile

device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers or cellular network; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol (“IP”) addresses and other information both in computer data format and in written record format.

26. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user’s true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.
27. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person “deletes” a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or

remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

28. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
29. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
30. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in **Attachment C**.
31. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as “apps,” are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such “apps” include Facebook, Telegram, LiveMe, Kik messenger service, Snapchat, Meet24, and Instagram.

32. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.
33. Individuals can also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Gmail, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or mobile device capable of accessing the Internet. Apps related to this cloud-storage accounts can also be downloaded to a computer or mobile device, allowing easier access to the content of the accounts.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

34. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
- A. Computer storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is

included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

B. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

35. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).
36. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices (including internal storage such as SD cards), any monitors, keyboards, and/or modems are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2252, and 2252A – the distribution, transmission, receipt, and/or possession of child pornography, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

37. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- 1) Examination of all of the data contained in such computer hardware, computer

software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in **Attachment C**;

- 2) Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in **Attachment C**;
- 3) Surveying various files, directories and the individual files they contain;
- 4) Opening files in order to determine their contents;
- 5) Scanning storage areas;
- 6) Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment C**; and/or
- 7) Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment C**.

VII. INVESTIGATION AND PROBABLE CAUSE

38. On December 23, 2021, agents with the FBI in El Paso, Texas interviewed an individual named Aaron MAGANA after learning MAGANA had been identified as a target in a child exploitation case stemming from a lead with the FBI in Birmingham, Alabama.
39. After receiving his *Miranda* warnings, MAGANA made admissions to the agents he purchased child sexual abuse material (CSAM) from an unknown individual on the mobile application Telegram. In order to make these purchases, MAGANA admitted he would send a direct message to that individual via Telegram requesting the CSAM. In return, the unknown individual would send MAGANA screenshots of folders or a screenshot of another Telegram group and further instruct MAGANA to make a payment to the Paypal account linked to email address eduardo.echalico@gmail.com (ECHALICO) to gain access to the folder or Telegram group centered on child pornography.
40. The investigation revealed MAGANA purchased child pornography from ECHALICO on following dates: February 19, 2021, February 25, 2021, February 28, 2021, March 28, 2021, April 10, 2021, and September 19, 2021. Law enforcement learned MAGANA would pay ECHALICO approximately \$20 to \$25 United States currency (USD) for each link or folder he purchased containing CSAM.
41. During the course of the initial investigation into MAGANA by the FBI in El Paso, legal

process was served to PayPal. In response, PayPal provided the following information relating to the Paypal account attributed to email address eduardo.echalico@gmail.com:

Registered User: Eduardo Eneluna Echalico
Date of Birth: March 27, 1975
Telephone Number: +63 9275329453
Address: 312 Manapat Street 42, Pasay City,
Metro Manilla, PH 1306

42. Based on the information from PayPal, law enforcement also learned that between February 1, 2021 and September 26, 2021, ECHALICO received approximately 499 payments from individuals all around the world, totaling \$19,022.96 USD. Approximately 130 different individuals made the payments, some of which were for the purchase of child exploitation material.

43. On January 14, 2022, law enforcement served additional legal process to PayPal requesting transaction and subscriber information related to PayPal account transactions between ECHALICO and numerous PayPal account users who were believed to be purchasers of CSAM. Law enforcement identified these possible purchasers of CSAM based on their review of the “notes” section of payments received by ECHALICO within the PayPal responsive records which included notes such as “390gb and Asian,” “For videos payment,” “Here you go. For 5 channels,” “folder access,” “Chinese Mega,” and “Personal Collection.”

44. In response, PayPal provided transaction and subscriber information related to PayPal account users located both in the United States and outside of the United States. Responsive records included the identification of Patrick ARIAS with the following billing and identifying information:

Name: Patrick ARIAS
Date of Birth: March 13, 1995
Email Addresses: pariasphoto@gmail.com; winterconlove@gmail.com
Telephone Numbers: 917-396-8169, 201-241-2955, 954-687-3523
Address: 9935 164th Avenue, Howard Beach, New York 11414
6412 Pembroke Road, Miramar, Florida 33023

45. After learning a possible purchaser of CSAM, specifically ARIAS, lived in New York, FBI agents there were notified. On December 7, 2022, agents with the Brooklyn-Queens FBI office interviewed ARIAS. Upon arriving at his residence, law enforcement asked ARIAS if he knew why they would be there to which he admitted to “collecting child pornography”. In further conversation with ARIAS, ARIAS admitted to being “addicted”

to child pornography since approximately 2017 and actively possessing child pornography on his cell phone, an Apple iPhone 12 mini, and possibly his desktop. ARIAS advised law enforcement he used multiple online platforms to obtain CSAM, including Twitter, Telegram, ICQ, and Mega.

46. After ARIAS provided oral and written consents for his devices, agents performed a cursory review of the cell phone and observed a substantial number of images and videos depicting child pornography as well as several accounts which ARIAS subscribed too that were related to child exploitation material groups. Further review of ARIAS' desktop also yielded social media accounts which ARIAS had registered accounts with and within those, evidence related to his membership in numerous CSAM groups within those accounts was noted.
47. During the course of the investigation into ARIAS, a full forensic examination and analysis was performed on ARIAS' devices. In that review, agents noted the mobile chatting application Signal installed on his Apple iPhone 12 mini. Your affiant knows Signal to be an encrypted messaging service for instant messaging, voice, and video calls. The instant messaging function includes sending text, voice notes, images, videos, and other files. Communication may be one-to-one between users, or for group messaging. In addition, your affiant knows Signal notifies all users of any legal process served on their account by law enforcement, despite any requested non-disclosure orders.
48. In addition, in review of the official Signal website, specifically www.signal.org/legal, under the "Privacy Policy" for user notes, Signal advises its potential subscribers that "you register a phone number when you create a Signal account. Phone numbers are used to provide our Services to you and other Signal users. You may optionally add other information to your account, such as a profile name and profile picture. This information is end-to-end encrypted."
49. Within the Signal application installed on the Apple iPhone 12 Mini attributed to ARIAS, law enforcement noted a group dedicated to the exchange of child pornography. The group had no name attributed to it and an emoji of a football was designated as the group photograph. One of the users observed within this Signal group had the profile name "JOHNNY3DEEP" and law enforcement noted "JOHNNY3DEEP" had been an active member at the time the device was reviewed. Specifically, "JOHNNY3DEEP" had distributed approximately six videos of child exploitation material into the Signal group,

some of which depicted infant children being sexually abused. Approximately 222 videos of child sexual abuse material and approximately 13 images were distributed to the Signal group. A summary of some of those videos revealed the following:

- Attachment 1d72d518-7ed1-7a32-c32b-5a91f2c26393 contained a 47 second video which depicted an approximately two-year-old nude male child in a bath with only a chain and cross around his neck. In the bath with the prepubescent male minor was a nude adult male with a partially erect penis. Approximately 22 seconds into the video, the adult male is depicted using his hand to manipulate the penis of the prepubescent male child.
- Attachment a94416f7-ee6d-545f-f3a6-a7f3dc03ebd7 contained a 14 second video which depicted an approximately seven-year-old nude male child performing oral sex on the penis of an adult male. A zebra printed blanket and blue towel or sheet are visible in the background.
- Attachment fbb2d1b6-5ee5-62bc-cd13-541007ebc9b9 contained a 66 second video which depicted an infant sleeping with a pacifier in his/her mouth. It is unclear based on the angle of the video and the age of the minor child if the infant is a male or female. An erect male penis is observed masturbating over the infant and eventually ejaculating onto the infant while he/she sleeps.

50. Law enforcement also noted another member of the same Signal chat group who utilized the profile name “GINGERCUB” with the associated phone number of (909) 289-5466.

Law enforcement learned that the (909) 289-5466 telephone number was resolved to AT&T and sent legal process to AT&T requesting subscriber records for that number.

51. In response, AT&T provided the following subscriber information for the (909) 289-5466 telephone number:

Name:	Ryan Christopher Ramos (the SUBJECT PERSON)
Credit Address:	1020 Luxe Avenue Apartment 8410, Columbus, OH 43220 (the SUBJECT PREMISES)
Customer Since:	02/22/2020;
User Address:	2350 Sawmill Place Boulevard, Apartment 347, Columbus, OH 43235.

After learning that the “GINGERCUB” user was the **SUBJECT PERSON**, law enforcement in New York sent an investigative lead to your affiant in Columbus, Ohio.

52. Further investigation into the **SUBJECT PERSON** via FBI database checks revealed that in 2018, the **SUBJECT PERSON** had been identified as sending money via PayPal to an individual named Jason RUIZ, an identified possessor and distributor of child pornography. Further information on RUIZ revealed RUIZ had been arrested by the New York City Police Department on January 19, 2019 for violation of New York Penal Code

263.15, Promotion Sexual Performance of a Child Less than 17 Years of Age and New York Penal Code 263.11, Possession of an Obscene Sexual Performance of a Child. The investigation into RUIZ was initiated in 2018 after RUIZ had been identified as selling child pornography and receiving money for it via PayPal. At the time, the **SUBJECT PERSON** had been identified as one of the many individuals who had sent money to RUIZ for child exploitation material and his name had been documented in the FBI reports accordingly.

53. In review of the 2018 investigation into RUIZ, PayPal also provided additional information about the individuals who sent RUIZ money, including the **SUBJECT PERSON**. Your affiant was able to ascertain that PayPal, in response to legal process served in 2018, provided identifiers for the **SUBJECT PERSON** such as his name, date of birth, social security number, and address, which your affiant knows to be the **SUBJECT PREMISES**. PayPal also provided an additional telephone number and email address for the **SUBJECT PERSON** which was noted as (909) 556-4548 and Ryan.C.Ramos85@outlook.com.

54. On March 27, 2023, legal process was sent to PayPal for records regarding the following identifiers related to the **SUBJECT PERSON**:

Name:	Ryan Ramos
Telephone Number:	(909) 556-4548
DOB:	October 22, 1985
Email Address:	Ryan.C.Ramos85@outlook.com

In return, PayPal responsive records revealed that the **SUBJECT PERSON** sent two payments to RUIZ via PayPal, one on May 13, 2018 for \$120.00 and one on May 17, 2018 for \$400.00.³

55. A check with the Bureau of Motor Vehicles, revealed Ryan C. Ramos, the **SUBJECT PERSON**, with a date of birth of October 22, 1985, resides at the 1020 Luxe Avenue, Apartment #8410, Columbus, Ohio location, the **SUBJECT PREMISES**. A check with the Bureau of Motor Vehicles did not indicate any other individuals resided at that

³ Per review of the reports of the investigation into RUIZ, your affiant learned that RUIZ made admissions to selling child pornography. Your affiant also learned that the PayPal account that the **SUBJECT PERSON** made payments to was the designated account RUIZ used for his child exploitation transactions and this was confirmed via the notes section of RUIZ's PayPal account which included transaction notes such as "kik," "Tumblr," "for some Vids," and "Can you send me a few more webcam teen/preteen vids?"

address. Your affiant also learned that a 2022 gray Toyota Rav4, VIN 2T3P1RFV2NW306767 bearing Ohio license plate HLH2747, the **SUBJECT VEHICLE**, was registered to the **SUBJECT PERSON**.

56. Further open-source checks revealed that the **SUBJECT PERSON** was a registered nurse at Nationwide Children's Hospital and had been so employed there since April 2018. The checks also noted that he was simultaneously employed at The Ohio State University Wexner Medical Center and had been so employed there since May 2020.
57. Surveillance of the **SUBJECT PREMISES** in July 2023 revealed the **SUBJECT VEHICLE** parked in the parking lot of the **SUBJECT PREMISES**. Surveillance of the **SUBJECT PREMISES** in July 2023 also revealed the **SUBJECT PERSON** driving the **SUBJECT VEHICLE** to his place of employment at OSU Wexner Medical Center.
58. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, are located on/in the **SUBJECT PREMISES**, **SUBJECT VEHICLE**, and **SUBJECT PERSON**. Therefore, I respectfully request that this Court issue search warrants for the locations described in **Attachments A and B**, authorizing the seizure and search of the items described in **Attachment C**.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

59. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved seeking/soliciting, receiving, distributing, and/or collecting child pornography:
- Those who seek out, exchange and/or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.
 - Those who seek out, trade and/or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs,

magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- Those who seek out, trade and/or collect child pornography sometimes maintain hard copies of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- Those who seek out, trade and/or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and have been known to maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

60. Based on all of the information contained herein, I believe **SUBJECT PERSON**, residing at the **SUBJECT PREMISES** and driving the **SUBJECT VEHICLE** likely displays

characteristics common to individuals who access online child sexual abuse and exploitation material and make payments for the content they receive. In particular, the target of investigation was a user of an encrypted messaging app and a member of a group dedicated to the distribution and sharing of child exploitation material and further paid money to a known, identified, and self-admitted seller of CSAM on at least two separate occasions.

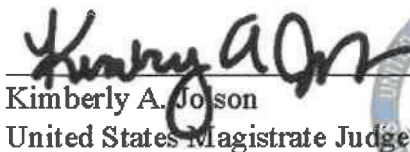
IX. CONCLUSION

61. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2252 and 2252A have been committed, and evidence of those violations is located in the **SUBJECT PREMISES** or **SUBJECT VEHICLE** described in **Attachment A** or on the **SUBJECT PERSON** described in **Attachment B**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in **Attachment C**.



Matthew W. Guinn
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 18th day of July, 2023.



Kimberly A. Tolson
United States Magistrate Judge

